Method for the Prevention of Erroneous Actuator Access in a Multifunctional General Electronic Control System

The present invention relates to a method for the prevention of erroneous actuator access in a multifunctional general electronic control system wherein the actuator access requirements emanate from different system services. The method is in particular appropriate for vehicle control systems.

Complex motor vehicle control systems are known in the art which integrate several functions such as anti-lock control (ABS), traction slip control (TCS), driving stability control (ESP), electrical overriding steering system, brake assist system, system or components diagnosis, etc. It is desired to use a joint electronic system in order to control these and other functions and auxiliary functions such as monitoring, error signaling, tire pressure monitoring, etc. The various functions and auxiliary functions are carried out or prepared to a large extent by means of the same actuators, such as pressure control valves, hydraulic pumps, warning lamps, etc. In this arrangement, the access to the individual actuators can definitely take place simultaneously. This will, of course, cause conflicts. It must be prevented that an access to an actuator is made by a control system or a control command of subordinate significance instead of a command that is more important at the moment e.g. due to safety reasons.

An object of the invention involves safeguarding that no 'erroneous', unauthorized access to an actuator takes place in a complex system of the above-mentioned type in the event of conflicting actuator access requirements. 'Erroneous' herein implies an access by a requirement which is instantaneously undesirable because a type of arbitration is demanded which is not allowable in the current mode of operation (e.g. a diagnosis measure during driving) or for various other reasons.

It has shown that this object can be achieved by the method described in claim 1, the special features of which reside in that a rights management, which determines the authorization of the system service for changing the instantaneous mode of operation of the general control system, a mode of operation control unit, and an access management are integrated into the system, in that the rights management in the event of an access requirement by the system service, brings about an adjustment or a change of the mode of operation according to predefined rules in consideration of the instantaneous general mode of operation of the general control system and reports the current mode of operation to the access management, and in that the access management, depending on the reported general mode of operation, allows only the 'authorized' system service to execute actuation of an actuator and processes the actuator access requirements of the system services according to predefined arbitration rules.

Thus, according to the invention, an additional rights and access management is integrated into the electronic control system of a multifunctional general control system, said management admitting access to the actuator of only those

access requirements of the various or different system services which are invariably predefined and 'desired' in the respective mode of operation. The access management gives preference or priority to those actions which must be preferred for safety reasons, for example.

The rights and access management of the invention renders it possible to integrate base functions and auxiliary or extraneous functions in a system without jeopardizing the base functions. The rights and access management is used to prevent that a brake actuation request which must have priority for safety reasons cannot be connected through e.g. due to an 'erroneous', unauthorized access to an actuator. Thus, only the invention renders it possible that several more important and, depending on the situation or mode of operation, less important functions can be integrated.

In a favorable embodiment of the method of the invention, the actuator access requirements of the system services are recorded in a memory and passed on to the access management separated according to types of arbitration.

A particularly favorable embodiment of the invention resides in that the actuator access requirement emanating from a system service and admitted to pass to an actuator is determined by a two-stage arbitration, i.e. a 'vertical' and a 'horizontal' arbitration.

In another embodiment of the invention, the unauthorized access requirements are determined, eliminated or rejected in the access management in a first step depending on the reported, current general mode of operation. In a second step, vertical arbitration is used to evaluate and select the

authorized access requirements according to a predefined order of priority of the types of arbitration, and higher priority is given to a 'current signal' rather than to a 'pressure signal', while higher priority is attributed to an 'ON/OFF signal' rather than to a current signal. Finally, in a third step, horizontal arbitration is used to evaluate and select the access requirements determined in the second step according to the priority of the signal by means of which the selected system service wants to drive the actuator.

It is expedient to write down the rights of the system services for a change of the mode of operation in a read-only memory to which the rights management has access, e.g. in the form of a table.

When the method of the invention is employed in a general control system for motor vehicles which, as a base system, comprises a brake system (EHB, EMB), the basic brake functions (BBF), wheel slip control functions (such as ABS, TCS, ESP), diagnosis functions (DIAG), motor pump control systems (MPA) and interfaces (BUS) are determined as system services from which actuator access requirements emanate, and checked by the rights management in connection with the access management.

Further system services such as 'customer software' (CSW), 'steering functions' (steer), etc., can still be integrated into the general system.

In a general control system for motor vehicles, a distinction is made in a favorable manner in the mode of operation control unit at least between the modes of operation 'normal operation' which occurs after termination of the starting phase in the absence of an error message, the mode of

operation 'starting phase' which applies e.g. until expiry of a predetermined period of time, until a minimum speed is reached for the first time, and/or until initial testing routines are completed, the mode of operation 'diagnosis', the mode of operation 'customer software' which is initiated in the case of an actuator access requirement by an extraneous or auxiliary system, and the mode of operation 'failsafe' indicating the presence of an error message.

Further features, advantages and possible applications of the invention can be seen in the following description of details of an embodiment by way of the accompanying drawings. In the drawings:

Figure 1 shows a schematic view of function elements of a general electronic control system for implementing the method of the invention;

Figure 2 shows also a schematic view of part of the general control system according to Figure 1 for illustrating the mode of operation of the access management.

The general control system which will be described as a simplified example in the following is intended for a motor vehicle with a complex brake system, such as an electrohydraulic brake system (EHB), being able to cooperate with systems and functions of most different types such as a brake assist system, speed control and collision avoidance control systems, diagnosis systems, steering systems (e.g. overriding steering system), etc. The brake system, including the associated control systems and functions ABS, TCS, ESP, etc., is considered as a base system, and the other systems or functions are considered as extraneous or auxiliary systems.

Figure 1 symbolically represents in a function block 1 those services, from which actuator access requirements originate which are 'managed' according to the method of the invention, that means checked with respect to their authorization. In the embodiment of the invention described herein, the services substantially are as follows, as is indicated in 1:

BBF refers to the basic brake function demanding an electronic control even in standard situations, e.g. in brake-by-wire systems (EHB; EMB);

ABS, TCS, ESP are control functions known by the name of these abbreviations;

DIAG refers to diagnosis functions;

MPA is the term for a motor pump assembly emanating from which are also actuator access requirements;

CSW symbolizes extraneous or auxiliary systems (CSW = Customer Software);

BUS refers to an interface such as a CAN-bus, through which, among others, access requirements of accessory functions or extraneous systems (CSW) are directed;

Steer refers to steering systems such as overriding steering systems.

Access requirements of collision avoidance systems (ACC), speed control systems (cruise control), etc., can also be integrated into the general control system by means of the system service 'BUS', through the interface CSW, or through another system service with an own identity (ID).

The actuator access requirements emanating from the system services 1 are checked in a rights management 2 with respect to being allowable or authorized in the current situation,

that means, in the instantaneous mode of operation (general mode of operation). A feedback from a mode of operation control unit 3 serves for this purpose.

Each service is definitely recognized by its ID. The following modes of operation which demand different reactions are e.g. of significance:

'normal' 'normal operation' is given e.g. after a longer period of operation of a motor vehicle without an error message;

'starting phase' applies, for example, as long as the individual systems are not yet in full function or routine checks have not yet been completed;

'diagnosis' this mode of operation prevails e.g. in the workshop or in the starting phase of the motor vehicle during the run of testing routines;

'CSW' customer software: this mode of operation is e.g. adjusted when the ID of the system service demanding access shows that the requirement does not originate from a base function, but from an accessory or auxiliary function or 'extraneous function';

'failsafe' an error was detected in the system causing service limitations.

The rules for judging the 'authorization' depending on the system service identified and the current mode of operation (general mode of operation) are invariably predefined. As shown in Figure 1, the rules are stored in a read-only memory 3, e.g. in tabular form, in the described embodiment of the invention.

The access requirement of the respective system service 1 is immediately rejected or ignored by the rights management 2 if no right to the actuator access requirement has been granted in the current general mode of operation. When the requirement in the current mode of operation is 'authorized', the mode of operation control unit 4 will trigger a change of the mode of operation of the general control system, if necessary. The current mode of operation is reported to an access management 6; further, feedback is given to the rights management 2.

The actuator access requirements of the individual system services 1 are sent to the access management 6 through the signal paths SD1 to SDn, simultaneously with the check of rights in the rights management 2, through an intermediate storage 5, said access management determining according to predetermined rules and controlled by arbitration which actuator access requirement of the system services 1 in the current mode of operation is actually allowed to pass until an actuator 7. All other requirements are ignored or rejected because of 'missing authorization'; the acceptance and/or the 'rejection' of the requirement being fed back to the system services 1.

As can be seen in Figure 2, the actuator access requirements are sorted in the intermediate storage 5 according to types of arbitration, that means, they are sorted according to signals of the same physical unit (herein: pressure 'p', current 'I', or ON/OFF signal 'E/A') and relayed to the access management.

In the access management 6, the requirements 'not authorized' in the current general mode of operation are rejected or eliminated in a first step. Subsequently, a two-stage arbitration of the remaining actuator access requirements

takes place. In a first step, symbolized by a block 8 in Figure 2, the 'authorized' requirements are evaluated according to a predetermined order of rank or priority of the individual types of arbitration; this is referred to as 'vertical' arbitration.

Subsequently, an evaluation of the remaining requirements of the same type of arbitration is carried out in a second step or a second stage 9 by 'horizontal' arbitration, and it is determined which one of the actuator access requirements is actually allowed to pass up to the actuator 7. Symbolized by a change-over switch 10, the output signal of the step 9 - depending on the type of arbitration, that means, herein 'pressure', 'current', or 'ON/OFF' signal - is passed on to the actuator 6 directly or after further processing in a pressure controller 11 and/or in a current controller 12.

In the embodiment of the invention described herein, the actuator 7 is a coil, e.g. the valve coil of a brake pressure control valve. A command or signal of the unit or dimension 'ON/OFF' causes a direct reaction of the valve. The 'ON/OFF' signal is therefore granted the 'highest' priority in the sense of the horizontal arbitration. A signal of the unit or dimension 'current', however, must initially be evaluated in a current controller 12 (see Figure 2) and converted into an 'ON/OFF' command. A pressure change requirement, meaning a signal of the dimension 'pressure', must first be converted into a current change requirement in a pressure controller 11 and thereafter converted into an actuator actuating signal or into an 'ON/OFF' signal by means of the current controller 12. A signal of the dimension 'current' is therefore given higher priority than a signal of the dimension 'pressure' in the present embodiment. With competing signals of the dimension

'pressure', 'current' and 'ON/OFF', the E/A signal is executed. In the absence of an E/A signal, the current signal is preferred.

The access management 6 selects the actuator access requirements according to predefined rules depending on the current mode of operation. For example, only pressure nominal value requirements are 'legitimate' in the mode of operation 'normal' and are evaluated; other requirements are rejected or ignored by the access management 6. In the mode of operation 'customer software' (CSW), only correcting commands or actuator access requirements in the form of pressure signals are permitted. In the mode of operation 'diagnosis', correcting commands in the form of current signals or valve alter statements rather than in the form of pressure signals are allowable. Only actuator requirements which emanate from the core system, covering above all the safety-critical system services, are 'legitimate' in the mode of operation 'failsafe', however, no actuator requirements of accessory systems, auxiliary systems of customer systems (CSW).

These are only relatively simple examples. A number of further specifications can be realized using the access management 6 in connection with the rights management 2 (3).